LISTING OF THE CLAIMS

1   1. (Currently Amended) A method for communication between two entities in a set of

2   clients across a network such that their identities are concealed from each other ~~and no~~

3   ~~third party is able to trace the communication~~ comprising the steps of:

4   providing a set of Forwarding Agents (FAs), there being n FAs and ~~several~~ a

5   plurality of groups of these n agents, each of which consists of a plurality of k members,

6   where k ~~($0 < k \leq n$)~~ is a fixed number considered sufficient to provide anonymity in the

7   system and each FA belongs to at least one group;

8   providing each of the FAs with its own pair of public and private keys for

9   encryption and decryption, respectively, where the underlying cryptosystem scheme is a

10   commutative public key cryptosystem, each FA also having appropriate keys required to

11   perform secure digital signatures on documents and to verify the signatures of other FAs;

12   registering each client with a Forwarding Agent S, the client once having selected

13   a Forwarding Agent S, ~~also~~ and picking one of the groups that the Forwarding Agent S

14   belongs to, thus selecting k agents to be associated with the client, the step of registering

15   including assigning a pseudonym X to the client and providing the Forwarding Agent S

16   with an encrypted form of the client's network address, the encrypted form being created

17   by successively encrypting by the client the client's network address with the public keys

18   of the k selected agents to obtain an encrypted address thereby rendering the network

19   address ~~it~~ unreadable to any individual FA;

20   maintaining by each FA a table with three fields, a pseudonym, a corresponding

21   encrypted network address and the FA group to be used for forwarding;

22   delivering a message meant for a pseudonym X to Forwarding Agent (FA) S

23   where X is registered using a protocol that protects the anonymity of the sender; and

24   passing the message through a random sequence of FAs in the group to which

25   Forwarding Agent S belongs until a FA in the group finds a visible network address and

1   then sending the message on to this address.

2   ; and

3   ——————finding by the last FA in the sequence a visible network address and sending the

4   message on to this address.

1   2. (Previously presented) A method for communication between two entities in a set of

2   clients across a network such that their identities are concealed from each other and no

3   third party is able to trace the communication comprising the steps of:

4   providing a set of Forwarding Agents (FAs), there being n FAs and several groups

5   of these n agents, each of which consists of k members, where k $(0 < k \leq n)$ is a fixed

6   number considered sufficient to provide anonymity in the system and each FA belongs to

7   at least one group;

8   providing each of the FAs with its own pair of public and private keys for

9   encryption and decryption, respectively, where the underlying cryptosystem scheme is a

10 commutative public key cryptosystem, each FA also having appropriate keys required to

11 perform secure digital signatures on documents and to verify the signatures of other FAs;

12 registering each client with a Forwarding Agent S, the client once having selected

13 a Forwarding Agent S, also picking one of the groups that the Forwarding Agent S

14 belongs to, thus selecting k agents to be associated with the client, the step of registering

15 including assigning a pseudonym X to the client and providing the Forwarding Agent S

16 with an encrypted form of the client's network address, rendering it unreadable to any

17 individual FA;

18 maintaining by each FA a table with three fields, a pseudonym, a corresponding

19 encrypted network address and the FA group to be used for forwarding;

20 delivering a message meant for a pseudonym X to Forwarding Agent (FA) S

21 where X is registered using a protocol that protects the anonymity of the sender;

22 passing the message through a random sequence of FAs in the group to which

23   Forwarding Agent S belongs; and

24   finding by the last FA in the sequence a visible network address and sending the

25   message on to this address, wherein the step of registering comprises the steps of:

26   successively encrypting by the client the client's network address with the public

27   keys of the k selected agents to obtain an encrypted address, referred to as the "onion

28   address" of the client;

29   sending by the client to the Forwarding Agent (FA) S a Registration Message

30   which contains the client's onion address and a chosen pseudonym X, and also identifies

31   the group of k agents selected by the client; and

32   adding by the Forwarding Agent the information contained in the Registration

33   Message to its table.

1   3. (Original) The method for communication recited in claim 2, wherein the Registration

2   Message is sent using a protocol which protects the anonymity of the sender.

1   4. (Original) The method for communication recited in claim 3, wherein the protocol

2   used comprises the Forwarding Agent (FA) S having a publicized pseudonym and the

3   client sending a message to that pseudonym.

1   5. (Previously presented) A method for communication between two entities in a set of

2   clients across a network such that their identities are concealed from each other and no

3   third party is able to trace the communication comprising the steps of:

4   providing a set of Forwarding Agents (FAs), there being n FAs and several groups

5   of these n agents, each of which consists of k members, where k $(0 < k \le n)$ is a fixed

6   number considered sufficient to provide anonymity in the system and each FA belongs to

7   at least one group;

8   providing each of the FAs with its own pair of public and private keys for

9   encryption and decryption, respectively, where the underlying cryptosystem scheme is a

10   commutative public key cryptosystem, each FA also having appropriate keys required to

11   perform secure digital signatures on documents and to verify the signatures of other FAs;

12   registering each client with a Forwarding Agent S, the client once having selected

13   a Forwarding Agent S, also picking one of the groups that the Forwarding Agent S

14   belongs to, thus selecting k agents to be associated with the client, the step of registering

15   including assigning a pseudonym X to the client and providing the Forwarding Agent S

16   with an encrypted form of the client's network address, rendering it unreadable to any

17   individual FA;

18   maintaining by each FA a table with three fields, a pseudonym, a corresponding

19   encrypted network address and the FA group to be used for forwarding;

20   delivering a message meant for a pseudonym X to Forwarding Agent (FA) S

21   where X is registered using a protocol that protects the anonymity of the sender;

22   passing the message through a random sequence of FAs in the group to which

23   Forwarding Agent S belongs; and

24   finding by the last FA in the sequence a visible network address and sending the

25   message on to this address, wherein once the Forwarding Agent (FA) S obtains a message

26   intended for X, the Forwarding Agent S performs the steps of:

27   looking up X in its internal table and retrieving an encrypted version of the

28   address of X, referred to as the "onion address" of X, as well as the group of FAs to be

29   used for forwarding;

30   creating the list of the FAs that the message will pass through, which list includes

31   all FAs other than S who will have to "peel the onion" before the address of the intended

32   recipient is revealed, the list containing all the members of the appropriate group except

33   the Forwarding Agent S itself; and

34   affixing the list to the head of the message.

1   6. (Original) The method of communication recited in claim 5, further comprising the

2   step of encrypting the message before forwarding it to FAs in the sequence.

1   7. (Original) The method of communication recited in claim 6, wherein the step of

2   encrypting comprises the steps of:

3   splitting the message into blocks of a fixed size;

4   prefixing each block with a fixed number of random bits, producing blocks of a

5   larger size; and

6   encrypting each block of a larger size with the public key or shared symmetric key

7   of the intended recipient.

1   8. (Original) The method of communication recited in claim 6, wherein each FA which

2   receives the message performs some verifications to ensure protocol consistency by other

3   FAs.

1   9. (Original) The method of communication recited in claim 8, wherein the verifications

2   comprise the steps of:

3   checking by an agent whether it is the first agent to be visited in the current

4   domain and, if so, selecting at random a tag N which has not been recently used and

5   affixing the tag to the message header before passing the message on;

6   otherwise, finding out the name S of the first agent to receive this message in the

7   current domain;

8   verifying a signature of S on a first part of the signed sequence in the message

9   header and, if this verification succeeds, then verifying that every successive segment of

10   the signed sequence bears the valid signature of the agent named in the preceding

11   segment;

12   verifying that the last segment of the signed sequence contains the name of the

13 agent performing the verification, while the penultimate segment contains the name of the

14 agent from which the message was received;

15 verifying that the list of unvisited agents does not contain any agents named in the

16 signed sequence; and

17 if any of the verifications fail, aborting the current message.

1 10. (Original) The method of communication recited in claim 8, wherein the verifications

2 comprise the steps of:

3 computing the agent's own sequence number i in the path followed by this

4 message through the set of forwarding agents by subtracting the number of FAs in the list

5 of unvisited FAs from $k + 1$;

6 checking if i is 1 and, if i is 1, then sending a coordinating agent (CA) 0 a request

7 for a tag and receiving the tag N as well as the number $k - 1$, combined with N and signed

8 before passing the message on;

9 if the number i is found to be different from 1, then verifying the signature of CA

10 $(i - 2)$ mod r on the signed number in the message header and, if verification succeeds,

11 then verifying if the signed number is $k + 1 - i$ and, if the verification succeeds, sending

12 the numbers $k + 1 - i$ and N and the name of the previous FA to CA $(i - 1)$ mod r;

13 receiving a signed number and a signal from CA $(i - 1)$ mod r and verifying if the

14 signal is "OK" and, if so, verification is complete and the message is passed on; but

15 if any of the verifications fail, concluding that the protocol has not been executed

16 correctly and aborting the current message.

1 11. (Original) The method of communication recited in claim 10, wherein the CA, upon

2 receiving a request from some FA, referred to as P, for a tag, performs the steps of:

3 selecting a tag N and sending it to P;

4 combining the tag N with a number $k - j$, signing the result and sending the signed

5   number to P along with an "OK" signal;

6   waiting for a message about the tag N, and upon receiving such a message,

7   verifying if it came from the next CA referred to as D, and if the message did not come

8   from D, announcing a protocol violation in receiving tag N;

9   otherwise, verifying the message involves the number $k - 1$, and if this verification

10   fails, sending an "Abort" message to D; but

11   if the verification passes, sending to D an "OK" signal and the identity of P.

1   12. (Original) The method of communication recited in claim 10, wherein any CA other

2   than CA 0, upon receiving a message from some FA referred to as P, performs the steps

3   of:

4   finding a number j, a tag N, and the identity of P, the previous FA, in the message;

5   sending a message to the previous CA asking for the name of the corresponding

6   FA, for tag N, and number $j + 1$;

7   receiving a signal and a table from the previous CA, and verifying that the signal

8   is "OK" and the name is P, and if such verification fails, sending an "Abort" signal to P;

9   otherwise, verifying that the most recent request, if any, involving the tag N

10   involved the number $j + 1$, verifying that it is the $(k - j)^{th}$ CA, and if either of these

11   verifications fails, sending an "Abort" signal to P;

12   but if the verifications pass, combining $j - 1$ with N, signing the result and sending

13   the signed number to P along with an "OK" signal;

14   waiting for a message about the tag N, and upon receiving such a message,

15   verifying if it came from the next CA referred to as D, and if the message did not come

16   from D, announcing a protocol violation in writing tag N;

17   otherwise, verifying the message involves the number $j - 1$, and if this verification

18   fails, sending to D an "OK" signal and the identity of P.

1   13. (Original) The method of communication recited in claim 5, wherein a next FA is

2   chosen comprising the steps of:

3   checking by an agent if there are any more agents to be visited in the present

4   domain and, if not, then marking the present domain as visited and removing the signed

5   sequence from the message header;

6   choosing an unvisited domain at random and making it the present domain;

7   choosing an agent belonging to the current domain at random from the list of

8   unvisited agents and, following this, passing the message on to the chosen agent;

9   if, instead, the agent finds that not all the agents in the domain have been visited,

10   then choosing at random an unvisited agent belonging to the current domain;

11   combining the random number N with the name of the chosen agent and signing

12   the resulting plaintext; and

13   adding the plaintext and signature to the signed sequence, following which the

14   message is forwarded to the chosen agent.

1   14. (Original) The method of communication recited in claim 5, wherein a next FA is

2   chosen comprising the steps of:

3   choosing by a current forwarding agent an FA at random from the list of unvisited

4   FAs in the message header;

5   removing its own name from the list;

6   adding the signed number that it received from an appropriate coordinating agent

7   (CA) to the message header; and

8   forwarding the message to the next chosen agent.